OFFICE OF THE DIRECTOR
DEPARTMENT OF MOTOR VEHICLES
Audits Office
P.O. BOX 932328 MS H-230
SACRAMENTO, CA 94232-3280

April 24, 2009

Mr. Alan Carlson, Chief Executive Officer
Superior Court of California County of Orange
700 Civic Center Drive West
Santa Ana, CA 92701

File No: C-40-9070

Dear Mr. Carlson:

The Department of Motor Vehicles (DMV) Audits Office presents its final audit report of the Superior Court of California of County of Orange (OCC) Audit for January 2007 – January 2009. The audit report entitled *"Final Audit Report – Superior Court of Orange County Audit"* is attached for your information. Please note the attached report includes excerpts of OCC response to our findings, as well as our evaluation to your response. We have included the response received from OCC in its entirety as an attachment at the end of the report.

The controls in place to protect DMV's record information are sufficient and functioning properly to fulfill the audit objectives. However, some DMV security requirements have not been adequately enforced. The findings are summarized as follows:

- Incomplete Log Maintained
- Security Violations – No Security Policies/Procedures for Protection of DMV Information
- Security Statements Violation – Failure to Maintain Information Security Statements for Employees

In addition, to the due dates identified in the "Audit Office Response" for each finding; at six months (October 2009), and again at one year (April 2010) from the date of this report, we request that OCC provide us with a written status on the corrective actions planned and/or implemented to address the reported findings.

We thank OCC and their staff during this review for their cooperation and courtesy extended to our auditors. If you have any questions, please contact me at (916) 657-5828.

Sincerely,

[redacted]

GRACE M. RULE-ALI, Manager
Information Systems-Requester Audit Section
(916) 657- 5828

Attachments

cc: Teresa Risi, Chief of Operations, Orange County Superior Court (OCSC)
Cherie Garofalo, Executive Director, Criminal Operations, OCSC
Tricia Penrose, Branch manager, HJC, OCSC
Gina Mendoza, Operations compliance Manager, OCSC
Paulette Johnson, Chief, Information Security and Privacy Officer, DMV
Stacy Cockrum, Chief, Information Services Branch, DMV

FINAL AUDIT REPORT

CALIFORNIA DEPARMENT OF MOTOR VEHICLES

SUPERIOR COURT OF ORANGE COUNTY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The California Department of Motor Vehicles (DMV) Information Services Branch operates an information requester program pursuant to California Vehicle Code (CVC) 1808.21 et seq., and Title 13, Division 1, Chapter 1, Article V, of the California Code of Regulations. As an authorized DMV Government Requester Account holder, Superior Court of Orange County (OCC) has access to California driver license and vehicle registration records. In accordance with its DMV Memorandum of Understanding (MOU), OCC is allowed to process California DMV inquiries for its business needs.

The California Vehicle Code requires that the Department protect the privacy rights of the public by releasing only certain information authorized by statutes. Statutes and regulations allow for businesses and individuals to access DMV records containing both confidential and non-confidential information, contingent upon approval of an application and compliance with the program requirements. To meet our obligation of protecting the public and DMV information, we audited OCC for compliance to the *Government Agency Requester Account Agreement, County Data Center/Court End User On-Line Access MOU and the California DMV Government On-Line Security Requirements,* standards developed by the *National Institute of Standards and Technology* (NIST), and other California law and regulations. This included a review of the DMV data security environment of OCC. The audit fieldwork was conducted January 28-29, 2009, at the OCC offices in Santa Ana and Newport Beach, California.

We evaluated the legitimacy of the requests, proper access, use, record maintenance, adequate management, administrative security procedures and security controls in place to protect the DMV record information. Our evaluation found that current security controls in effect as of January 29, 2009, are sufficient to meet the security objectives of this audit, except as noted in the *Findings and Recommendations* section of this report however, they are summarized below:

- Incomplete Log Maintained.
- Security Violations - No security policies/procedures for protection of DMV information.
- Security Statements Violations - Failure to maintain Information Security Statements for employees.

BACKGROUND

DMV is responsible for administering statewide programs that use and rely on electronically stored and hard copy information assets. A structure of laws, regulations, and administrative requirements, along with information security requirements and practices determine the

permissive uses and necessary protection of this information. DMV also conducts audits and evaluations of entities accessing the information of the Department, to ensure that these entities abide by the applicable laws and regulations and/or other departmental requirements.
OCC has been a DMV Government Requester Account holder since 1991. In 2002, OCC was approved for on-line access to DMV via the Orange County General Services Agency Information Services referred to as County Data Center (CDC). Users are required to key data 1 into formatted fields to complete a DMV request. Currently, OCC has approximately 500 DMV users.

In July 2007, DMV's Information Services Branch (ISB) requested an audit of OCC. An article in the Orange County Register stated OCC had contracted with a company in Mexico to process data entry of traffic tickets. Information from tickets included driver license numbers, vehicle registration numbers, addresses, and birth dates. ISB was concerned OCC's contracting out to a source in Mexico may be a violation of their DMV agreement. The OCC later issued a press release stating they no longer outsource to Mexico.

During the audit we confirmed that effective August 3, 2007, OCC amended their contract with Cal Coast Data Entry, Inc. (CCDE), to process traffic data entry to be done at their Cerritos, California and at their Phoenix, Arizona facilities. Records are no longer being sent to Nogales, Mexico for data entry.

The *Government Agency Requester Account Agreement, County Data Center/Court End User On-Line Access MOU, and the California DMV Government On-Line Security Requirements,* and standards developed by the *National Institute of Standards and Technology* (NIST), are the primary criteria for this review. The fieldwork of OCC was conducted January 28, through January 29, 2009.

SCOPE AND OBJECTIVES

The audit objectives were to 1) verify compliance with the requirements of the MOU and the California DMV Government On-Line Security Requirements, as well as applicable statues and regulations stated in the California Vehicle Code, and the California Code of Regulations; and 2) review the security procedures that OCC has in place to ensure the protection of DMV information. This included evaluation of OCC levels of access controls; physical security access controls requirements, and administrative policies and procedures.

The information presented in this report was gathered during our fieldwork at the OCC on January 28-29, 2009, at Santa Ana and Newport Beach, California for requester codes [redacted]. This audit was conducted in accordance with *Government Auditing Standards* promulgated by the United States General Accountability Office. Our evaluation methodology included such tests as considered necessary to meet our objectives. Our procedures included interviews with OCC staff and management, physical observation of the OCC facilities and operations, review and verification of available system documentation, and testing to determine the levels of security and confidentiality over DMV information.

Our evaluation revealed that current security controls in effect at OCC as of January 29, 2009, are sufficient to meet the security objectives of this review, except as noted in the *Findings and Recommendations* section of this report. However, because of inherent limitations in control systems, error or irregularities may occur and not be detected. Therefore, projection of any evaluation of systems to future periods is subject to risk because procedures may become inadequate due to changes in conditions, or degree of compliance with the procedures may deteriorate.

FINDINGS AND RECOMMENDATIONS

FINDING #1: INCOMPLETE LOG MAINTAINED

Condition: During the audit period January 2007 through January 2009, OCC did not maintain an adequate transaction log that contained the required elements in accordance with their MOU. The current log maintained by OCC did not contain the information codes and all of the individual user identifiers, including individual user ID.

The transaction log is essential for OCC to properly monitor their account activity, and to maintain documentation of DMV information request. The transaction log provides audit trail information and must be preserved and available for audit purposes when requested by DMV.

The transactions log captures information on why a DMV inquiry was made, who requested the information, what information was requested, where the request was initiated and when the information was requested.

Criteria: The County Data Center/Court End User On-Line Access (Inquiry/Update) MOU #17 states in part that "...The information shall be preserved for audit purposes and must include, at a minimum, the following:

a. Transactions and information codes
b. Requester code
c. Record identifiers
d. All individual user identifiers, including individual user ID

California Code of Regulations Section 350.48(c) states in part, "Each requester code holder who is requesting or receiving confidential information...shall maintain a monthly record of each request for information for a period of two (2) years from the date of the request, showing the date of the request, the requester code of the person making the request to the department, the type of information requested (vehicle or vessel registration, drivers license, financial responsibility, or occupational licensing), points of identification used for the request (e.g., license number and date of birth), and the purpose of the request, in that order."

Recommendation: OCC should ensure that the transactions log include all of the required elements identified in the MOU. It is suggested that the OCC conduct a period review of the transactions log to verify that that all of the required elements are being captured.

Court Response: "Concur and corrective action will be taken. The court will ensure that the transactions log includes all required elements as identified in the MOU by May 2009. Additionally, ...will regularly review the transactions log to verify compliance ..."

Audit Office Response: We concur with OCC corrective action plan. To evidence compliance in this area, we ask that OCC submit a written status report by May 29, 2009.

FINDING #2: SECURITY VIOLATIONS – NO SECURITY POLICIES/PROCEDURES FOR PROTECTION OF DMV INFORMATION

Condition: OCC did not maintain security polices and procedures for protection of DMV information. Employees are unaware of DMV's security policies/procedures for protecting DMV data.

An information security program provides OCC the ability to establish guidelines intended to adequately protect DMV data. The information security program provides employees with policies, procedures, guidelines, security awareness and training programs necessary for the protection of DMV's data.

Criteria: California Vehicle Code Section 1808.47 states in part, "Any person who has access to confidential or restricted information from DMV shall establish procedures to protect the confidentiality of those records." Commercial Requester Information Handbook, Chapter Two, Part VI, Answers to Questions 8, 9 and 10 states in part, You are required to establish written procedures to protect the confidentiality of the information received from DMV. The established security procedures must be maintained on site and available to the department's auditors." In order to adhere to this requirement OCC should appoint someone to be in charge of maintaining the security of DMV information.

Recommendation: Develop security policies and procedures for protection of DMV data. Refer to the California DMV Government On-Line Security Requirements, and standards developed by NIST. OCC should develop policies and procedures to ensure employees with direct and incidental access to DMV information are aware of the requirements for protection of DMV data.

Court Response: "Concur and corrective action will be taken. The Court will develop and maintain written procedures...by July 2009...Comprehensive, court wide training will be conducted...Court's compliance unit will assume responsibility for maintaining procedures and regularly auditing staff compliance with applicable requirements."

Audit Office Response: We concur with OCC corrective action plan. To evidence compliance in this area, we ask that OCC submit a written status report by July 30, 2009.

FINDING #3: SECURITY STATEMENTS VIOLATIONS – FAILURE TO MAINTAIN INFORMATION SECURITY STATEMENTS FOR EMPLOYEES

Condition: The OCC did not maintain Information Security Statements (INF 1128), for all account users. All OCC employees, and/or system administrators with direct of indirect access to DMV information must sign statements, and recertify annually. The security statements record that OCC employees are informed to restrict the use and knowledge of requester codes, operational manuals, and DMV information to those who are authorized.

Criteria: The County Data Center/Court End User On-Line Access (Inquiry/Update) MOU # 9 states, "Requester agrees to establish security procedures to protect the confidentiality of DMV records and access information, as required by California Vehicle Code Section 1808.47. Requester shall ensure that each Requester's employee or each person working on behalf of Requester having direct or incidental access to DMV records have signed an individual security statement. That statement shall contain, at a minimum, the same provisions contained within the DMV's Information Security Statement, form INF 1128. The form shall be maintained on file, and made available to DMV upon request".

Recommendation: OCC should develop policies and procedures to ensure that all employees with direct and incidental access to DMV records information sign and maintain at worksite, INF 1128, and recertify annually.

Court Response: "Concur and corrective action will be taken. The Court has begun efforts to implement a training component...to capture all staff that will have direct or incidental DMV access....Additionally, each new employee will be required to review and sign form INF 1128 and will recertify each employee annually...This action will occur by July 2009."

Audit Office Response: We concur with OCC corrective action plan. To evidence compliance in this area, we ask that OCC submit a written status report by July 30, 2009.

OBSERVATION

OCC does not have a method in place to monitor user activity to provide reasonable assurance that the information requests are associated with legitimate court business. To reduce the risk of inappropriate activities OCC should increase oversight of user activity by implementing monitoring controls to deter unauthorized activity by system users. Consider methods to monitor user activity on a regular basis. Such methods could include generation and review of exception reports, user activity reports or system activity reports including software to electronically monitor and track user activity.

CONCLUSION

OCC operates a system and program designed to provide DMV record information to conduct legitimate court business. The on-line DMV requirements are to establish requirements for security features to authenticate authorized users and have adequate security controls in place to protect DMV data. The physical access control requirements have security features in place to protect the physical environment where DMV record information is stored.

We concur with OCC corrective action plan. Implementation of the Recommendations identified will provide mechanisms and controls to protect DMV information. We will be expecting status reports as identified in the "Audit Office Response" of each finding. In addition, status reports at six months (October 2009) and in one year (April 2010). However, because of inherent limitations in controls systems, errors or irregularities may occur and not be detected. Therefore, projection of any evaluation of systems to future periods is subject to risk because procedures may become inadequate due to changes in conditions, or the degree of compliance with the procedures may deteriorate.

[redacted]

GRACE M. RULE-ALI, Manager
Information Systems-Requester Audit Section
Audits Office
(916) 657-5828

February 27, 2009

Review Team:
Laura Lundgren, Supervisor
Carolyn Manuel, Auditor

Superior Court of California
County of Orange

CARLSON, ALAN
CHIEF EXECUTIVE OFFICER
CLERK OF THE COURT
JURY COMMISSIONER

700 CIVIC CENTER DRIVE WEST
SANTA ANA, CALIFORNIA 92701
PHONE: 714-834-5277
FAX: 714-568-5784

April 6, 2009

Department of Motor Vehicles
Audit Office
2570 24th Street, MS H121
Sacramento, CA 95818

Attention: Carolyn Manuel, Auditor

Subject: Response to Draft Audit Report entitled 'Superior Court of Orange County Audit'

In response to your letter dated March 23, 2009, included are the responses from the Superior Court of California County of Orange, to the findings contained in your draft report entitled *'Superior Court of Orange County Audit'*.

The following are brief summaries of each finding, a summary of each recommendation and a court response to each of one of the findings.

Finding #1: INCOMPLETE LOG MAINTAINED

Recommendation: OCC should ensure that the transactions log include all of the required elements identified in the MOU. It is suggested that the OCC conduct a period review of the transactions log to verify that all of the required elements are being captured.

Court Response: Concur and corrective action will be taken. The court will ensure that the transactions log includes all required elements as identified in the MOU by May 2009. Additionally, the Court's Compliance Unit will regularly review the transactions log to verify compliance with requirements and will make the logs readily available to the Department of Motor Vehicles (DMV) upon request.

Finding #2: SECURITY VIOLATIONS – NO SECURITY POLICIES/PROCEDURES FOR PROTECTION OF DMV INFORMATION

Recommendation: Develop security policies and procedures for protection of DMV data. Refer to the California DMV Government On-Line Security Requirements, and standards developed by NIST. OCC should develop policies and procedures to ensure employees with

direct and incidental access to DMV information are aware of the requirements for protection of DMV data.

Court Response: Concur and corrective action will be taken. The Court will develop and maintain written procedures in accordance with the requirements set forth by the Department of Motor Vehicles by July 2009. Comprehensive, court-wide training will be conducted to ensure that all staff with direct and incidental access becomes familiar with the procedures in order to protect the confidentiality of the information received from DMV. Additionally, the Court's Compliance unit will assume responsibility for maintaining procedures and regularly auditing staff compliance with applicable requirements.

Finding #3: SECURITY STATEMENTS VIOLATIONS – FAILURE TO MAINTAIN INFORMATION SECURITY STATEMENTS FOR EMPLOYEES

Recommendation: OCC should develop policies and procedures to ensure that all employees with direct and incidental access to DMV records information sign and maintain at worksite, INF 1128, and recertify annually.

Court Response: Concur and corrective action will be taken. The Court has begun efforts to implement a training component during New Employee Orientation to capture all staff that will have direct or incidental DMV access. The program will provide staff with an overview of policies and procedures aimed at protecting DMV information. Additionally, each new employee will be required to review and sign form INF 1128 and will recertify each employee annually, as required by the MOU and Vehicle Code Section 1808.47. This action will occur by July 2009.

The Court is currently reviewing a list of all existing employees and will ensure that they receive appropriate training and sign form INF 1128 or recertify as applicable. The Court's Compliance unit will maintain INF 1128 forms for all employees with direct or incidental access to DMV and will make these records available at the request of the DMV. This action will occur by May 2009.

Sincerely,

[redacted]

Alan Carlson
Chief Executive Officer

cc: Teresa Risi, Chief of Operations, OCSC
Cherie Garofalo, Executive Director, Criminal Operations, OCSC
Tricia Penrose, Branch Manager, HJC, OCSC
Gina Mendoza, Operations Compliance Manager, OCSC